

January 8, 2019

**VIA CM/ECF**

Hon. Peter R. Marksteiner  
Circuit Executive & Clerk of Court  
United States Court of Appeals  
for the Federal Circuit  
717 Madison Place, N.W.  
Washington, D.C. 20439

**Re: *In re Google LLC*, No. 18-152**

Dear Colonel Marksteiner:

Pursuant to Federal Rule of Appellate Procedure 28(j), Google LLC writes to advise the Court that on December 21, 2018 a district court in the Northern District of Texas held that a company's "servers at a data center owned by a third party" do not "constitute[] a regular and established place of business." Order at 4, *CUPP Cybersecurity, LLC v. Symantec Corp.*, No. 3:18-cv-1554-M (Dec. 21, 2018) (Dkt. 44). While the district court subsequently vacated its order to determine whether the case should be transferred to the Northern District of California rather than Delaware, it did not signal any retreat from its holding that venue was improper in the Northern District of Texas. And that holding provides strong support for Google's petition for rehearing.

In its petition, Google asserted that there was a split among district courts as to whether a defendant who keeps computer servers in the facility of a third party in a judicial district has a "regular and established place of business" there under 28 U.S.C. § 1400(b). The decision in *CUPP* acknowledged and deepened the confusion, holding—contrary to the district court in this case—that "the relevant case law[] and the language of the statute" both dictate that a company's servers are not a "regular and established place of business." Order at 4-5.

In denying mandamus here, the panel suggested that the district court's decision was fact-bound. Panel Op. 4-5. But *CUPP* illustrates well the panel's error: It involves an entirely different company, and an entirely different plaintiff, but *precisely* the same legal question regarding the proper interpretation of the patent venue statute.

*En banc* or panel rehearing is urgently warranted. The trial in this case is scheduled to begin on January 21, 2019, and it will be followed by post-trial motions. That burdensome

litigation will take place in a district where venue is improper, while other district courts and litigants continue to wrestle with a clear split of authority on an important and recurring question. To avoid this needless waste of judicial resources, this Court should grant the requested mandamus relief as soon as possible.

Respectfully submitted,

/s/ Neal Kumar Katyal  
Neal Kumar Katyal

cc: All Counsel of Record (via CM/ECF)

### **CERTIFICATE OF SERVICE**

I certify that on January 8, 2019, I caused a copy of the foregoing document to be served by electronic means via the Court's CM/ECF system on all counsel registered to receive electronic notices.

/s/ Neal Kumar Katyal  
Neal Kumar Katyal

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION**

CUPP CYBERSECURITY LLC, et al.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	Civil Action No. 3:18-CV-01554-M
	§	
SYMANTEC CORPORATION,	§	
	§	
Defendant.	§	

**ORDER**

Defendant Symantec Corporation moves to dismiss this patent case for improper venue. Under 28 U.S.C. § 1400(b), a patent case may be brought in the judicial district where (1) the defendant resides, or (2) where the defendant has committed acts of infringement and has a regular and established place of business. Because Symantec does not reside in this District and Plaintiffs CUPP Cybersecurity, LLC and CUPP Computing AS (collectively, “CUPP”) have failed to show that Symantec has a regular and established place of business in this District, venue is not proper in the Northern District of Texas. The Court finds that the interest of justice is best served by transferring this case to the District of Delaware, where Symantec resides.

**I. Background**

CUPP brings this suit against Symantec, asserting that Symantec has directly and indirectly infringed eight of CUPP’s patents that cover software- and hardware-based solutions to problems in mobile device management, network security, demilitarized zone security, and endpoint security.

On August 6, 2018, Symantec moved to dismiss the case for improper venue under Federal Rule of Civil Procedure 12(b)(3), or in the alternative, for transfer to the Northern

District of California. (ECF No. 31). CUPP responded on August 27, 2018, arguing that venue is proper in this District. (ECF No. 34). In the alternative, CUPP requests venue-related discovery or transfer to the District of Delaware. (*Id.*). On September 10, 2018, Symantec filed a Reply (ECF No. 36) and a Motion for Leave to File Appendix in Support of Reply (ECF No. 38). The Motion for Leave to File Appendix in Support of Reply is GRANTED. Symantec's Motion to Dismiss for Improper Venue is ripe for review.

## **II. Legal Standard**

Venue in a patent infringement action is governed by a special patent venue statute, which provides that a patent infringement case may be brought in the judicial district where (1) the defendant resides, or (2) where the defendant has committed acts of infringement and has a regular and established place of business. 28 U.S.C. § 1400(b). The Supreme Court has stated that, for purposes of the patent venue statute, a domestic corporation “resides” only in its state of incorporation. *TC Heartland LLC v. Kraft Foods Grp. Brands LLC*, 137 S. Ct. 1514, 1519 (2017). The inquiry into whether a defendant has a “regular and established place of business” has three general requirements: “(1) there must be a physical place in the district; (2) it must be a regular and established place of business; and (3) it must be the place of the defendant.” *In re Cray Inc.*, 871 F.3d 1355, 1360 (Fed. Cir. 2017).

The Federal Circuit has not ruled on which party bears the burden of proof in a § 1400(b) matter. But district courts have imposed the burden of proving that venue is proper on the plaintiff once a defendant has objected to the plaintiff's chosen forum. *See, e.g., Galderma Labs., L.P. v. Teva Pharm. USA, Inc.*, 290 F. Supp. 3d 599, 606 (N.D. Tex. 2017); *Personal Audio, LLC v. Google, Inc.*, 280 F. Supp.3d 922, 926 (E.D. Tex. 2017).

### **III. Analysis**

#### **A. Venue in the Northern District of Texas is Improper.**

Because Symantec is incorporated in Delaware, the first prong of § 1400(b) cannot be satisfied. Thus, venue is proper in this District only if Symantec (a) has committed acts of infringement in this District and (b) has a regular and established place of business in this District. 28 U.S.C. § 1400(b). CUPP argues that Symantec has a regular and established place of business, because Symantec has data centers, employees, and offices in the Northern District of Texas.

##### **1. Data Centers**

CUPP asserts venue is proper because Symantec “has at least two different data centers in this District to host its Web Security Service (‘WSS’) product.” (ECF No. 34 at 2). CUPP provides the following evidence in support:

- Symantec’s WSS Registration and Admin Guide lists the Virtual IP Addresses and Authentication IP Addresses associated with each of Symantec’s WSS data center locations, including a location in Dallas, Texas. (ECF No. 35 at App. 035–038).
- A website maintained by Symantec that displays the “real-time performance of its data centers” includes a data center in Dallas, which is abbreviated as “DA1.” (*Id.* at App. 043; EFC No. 34 at 2).
- A website maintained by Symantec published a “Network Maintenance Notification” for “Dallas (DA1)” to Symantec’s customers on August 16, 2018. (ECF No. 35 at App. 045).
- A website maintained by Symantec published a notice stating “Customer connections to the Dallas data center may be experiencing increased latency.” (*Id.* at App. 047).
- Symantec published an online article on June 22, 2018, titled, “Data center IP addresses for Web Security Services (WSS),” which lists an IP address for “[DA1/DFW2]” database in Dallas. (*Id.* at App. 023).

- CUPP conducted a search of “DA1” on a search engine called “Cloudscene” and determined that the “DA1” data center is operated by Equinix and is located at 1950 Stemmons Freeway in Dallas. (*Id.* at App. 057–061, 068).
- CUPP searched the “DFW2” acronym on Cloudscene and found two data centers: (1) “DFW2” is operated by Atlantic Metro Communications and is located in Dallas, Texas, and (2) “DFW-2” is operated by DataBank and is located in Richardson, Texas. (*Id.* at App. 069–073).

Symantec responds that it only has servers at one data center in Dallas: the DA1 data center operated by Equinix. (ECF No. 36 at 7; ECF No. 37 at App047–053). Symantec states it does not have “any equipment or operations” at the data center operated by DataBank, Ltd., known as “DFW-2,” or at the data center operated by Atlantic Metro Communications II, Inc., known as “DFW2.” (ECF No. 37 at App047–048 ¶¶ 4–5).

Based on the evidence before it, the Court finds that CUPP has shown—and Symantec does not dispute—that Symantec has servers at an Equinix data center known as “DA1” in Dallas, Texas. CUPP has failed to show that Symantec has servers at any other location in this District. CUPP’s searches on Cloudscene do not prove that Symantec has servers at the DFW2 or DFW-2 data centers operated by Atlantic Metro Communications and DataBank, respectively. Further, despite CUPP’s continual reference to “Symantec’s datacenter,” the evidence shows that Symantec does not own the data center, but that “Symantec has an agreement with [Equinix] that allows Symantec to co-locate its servers at an Equinix datacenter . . .” (*Id.* at App048 ¶ 6). Thus, the issue is whether the presence of Symantec’s servers at a data center owned by a third party constitutes a regular and established place of business.

The Federal Circuit has not yet determined whether the presence of a company’s servers in a data center operated by a third party establishes a regular and established place of business for purposes of venue. The Court is aware that district courts within the Fifth Circuit addressing this issue have come to conflicting conclusions. *Compare Personal Audio, LLC v. Google, Inc.*,

280 F.Supp.3d 922, 934 (E.D. Tex. 2017) (determining that Google’s servers hosted in third-party server rooms do not establish a regular and established place of business) *with Seven Networks, LLC v. Google LLC*, 315 F.Supp.3d 933, 966 (E.D. Tex. 2018) (concluding that Google’s servers hosted in third-party server rooms do establish a regular and established place of business).<sup>1</sup> After considering the parties’ arguments, the relevant case law, and the language of the statute, the Court finds that Symantec’s servers do not constitute a regular and established place of business in this District.

The first requirement of whether a defendant has a regular and established place of business is that there “must be a physical place in the district.” *In re Cray*, 871 F.3d at 1360. The statute requires a “‘place,’ *i.e.*, ‘[a] building or a part of a building set apart for any purpose’ or ‘quarters of any kind’ from which business is conducted.” *Id.* at 1362 (internal citation omitted). “The statute thus cannot be read to refer merely to a virtual space or to electronic communications from one person to another.” *Id.* Symantec’s servers are not a building or a part of a building. Servers are “‘hardware,’ the physical electronic equipment used to operate the internet or an intranet.” *Personal Audio, LLC*, 280 F.Supp.3d at 934. The business conducted from Symantec servers involves “electronic communications,” which the Federal Circuit specifically stated cannot constitute a place. *In re Cray*, 871 F.3d at 1362.

With respect to the second requirement that the place “must be a regular and established place of business,” the Federal Circuit has stated that the place must be operating in a “steady, uniform, orderly, and methodical manner.” *Id.* at 1363 (internal citation and quotation omitted).

---

<sup>1</sup> In *Seven Networks, LLC*, Google filed a petition for a writ of mandamus, requesting that the Federal Circuit direct the Eastern District of Texas to find that Google’s servers did not establish a regular and established place of business and to dismiss or transfer the case under § 1400(b). *In re Google LLC*, 2018-152, 2018 WL 5536478 (Fed. Cir. Oct. 29, 2018). The Federal Circuit denied the petition without deciding the merits. *Id.* at \*3. Judge Reyna filed a dissent. *Id.* at \*4.



“[T]he defendant must actually engage in business from that location.” *Id.* at 1364. *See Peerless Network, Inc. v. Blitz Telecom Consulting, LLC*, Case No. 17-cv-1725, 2018 WL 1478047, at \*4 (S.D.N.Y. Mar. 26, 2018) (A place of business “is a location where, for example, products are made, customers are served, or business decisions are made.”). Symantec’s WSS product is a “cloud-based product” that allows Symantec customers to direct traffic through Symantec’s servers. (ECF No. 35 at App. 032–035). The servers themselves are not places from which Symantec conducts its business. As the court found in *Personal Audio*, to conclude that a company’s business is being carried out by its servers,

would have far-reaching consequences that distort the scope of the statute; for example, every single AT&T tower would then possibly become a place of business for AT&T. Maybe even every handheld device sold by Verizon would become a place of business for Verizon because the end-user signed an agreement with Verizon regarding Verizon’s exclusive control of the device.

280 F.Supp.3d at 934.

Because Symantec’s servers do not satisfy the first two requirements of whether Symantec has a “regular and established place of business,” the Court need not consider the third requirement. CUPP has failed to meet its burden to prove that Symantec’s servers constitute a “regular and established place of business” in this District.

## **2. Employees**

CUPP argues that Symantec has employees in the Northern District of Texas and “these employees are likely to have home offices or other office space in this District paid for by Symantec.” (ECF No. 34 at 3, 10). For support, CUPP cites to the LinkedIn profiles of Symantec’s President and COO, Michael Fey; Chief Marketing Officer, Michael Williams; and Chief Strategy Officer, Brian Kenyon. (ECF No. 35 at App. 084–092). On each of these three profiles, it states “Dallas/Fort Worth Area” under each person’s title. (*Id.*). CUPP provides a

document that appears to be the profile of an unnamed employee who was the “Large Enterprise Sales Manager” from January 2006 to February 2013 at Symantec and “led a Large Enterprise team in the DFW, Arkansas, and Oklahoma markets. This team was responsible for selling all Symantec products and services to the largest customers in this territory.” (*Id.* at App. 094). CUPP also submits a screen shot of the results of a LinkedIn search that shows six job listings for Symantec in “Dallas, TX, US.” (ECF No. 34 at 4).

CUPP’s argument that venue can be based on Symantec employees working in this District does not satisfy the first requirement that “there must be a physical place in the district.” *In re Cray*, 871 F.3d at 1360. There is no evidence that any of the Symantec employees that CUPP discusses have a home office in this District.

Even if the record showed that Symantec employees had home offices within the District, CUPP has failed to establish that those home offices would be “place[s] of the defendant,” as necessitated by the third requirement. As the Federal Circuit stated in *In re Cray*, the defendant “must establish or ratify the place of business.” *Id.* at 1363. In making this determination, relevant considerations include (1) “whether the defendant owns or leases the place, or exercises other attributes of possession or control over the place;” (2) “whether the defendant conditioned employment on an employee’s continued residence in the district or the storing of materials at a place in the district so that they can be distributed or sold from that place;” (3) “whether the defendant lists the alleged place of business on a website, or in a telephone or other directory;” and (4) whether the defendant “places its name on a sign associated with or on the building itself.” *Id.*

CUPP presents no evidence that any of Symantec’s employees who live in this District have a home office owned, leased, or otherwise controlled by Symantec. On the other hand,

Symantec submits evidence that it has 149 remote employees, including Michael Fey, Michael Williams, and Brian Kenyon, who choose to, but are not required to, live in Texas. (ECF No. 37 at App057 ¶ 4). Symantec does not condition its remote workers' employment on the workers storing, distributing, or selling materials from their homes in this District. (*Id.* at App041–046). Symantec's policy specifically prohibits remote employees from conducting "in-person business meetings of any nature or host[ing] visitors for business purposes (during business hours) at their home or remote offices." (*Id.* at App071). Symantec shows that it does not own or lease any remote employees' homes or provide housing allowances to remote employees in Texas. (*Id.* at App041–50, 56–57, 72). Further, Symantec presents evidence that the job listings cited by CUPP state the job location as "USA- Texas, Remote" or as other cities outside of this District. (*Id.* at App079–137). As in *In re Cray*, the evidence does not show that Symantec's remote employees' location in the Northern District of Texas was "material" to Symantec's business. *See* 871 F.3d at 1365. It is not enough to show that "there exists within the district a physical location where an employee of the defendant carries on certain work for his employer." *Id.* at 1366. CUPP has failed to establish that Symantec maintains a regular and established place of business in the Northern District of Texas based on any Symantec employees who work or have a home office within the District.

### **3. Offices**

CUPP claims that Symantec has a regular and established place of business in this District because it has offices at five addresses in Dallas: 15950 Dallas Pkwy #800, Dallas, Texas 75248; 5015 Addison Circle, Addison, Texas 75001; 600 Six Flags Dr., Ste 650, Arlington, Texas 76011; 15851 Dallas Pkwy, Ste 1103, Addison, Texas 75001; and 17250 Knoll Trail Dr., Dallas, Texas 75248. (ECF No. 34 at 12). CUPP appears to have found the 15950

Dallas Pkwy address through a general internet search. (ECF No. 35 at App. 095–098). CUPP found the 5015 Addison Circle, 600 Six Flags Dr., and 15851 Dallas Pkwy addresses by running credit reports on Symantec. (*Id.* at App. 099–107). CUPP found the 17250 Knoll Trail Dr. address through a Google Maps search for “Symantec Corporation.” (*Id.* at App. 111–14).

Symantec responds that it has no offices in the Northern District of Texas. (ECF No. 32 at Appx006 ¶ 5). Symantec states that it previously leased an office at 15950 Dallas Pkwy and that the office was occupied by Veritas Technologies Corporation, a company Symantec had merged with in 2005. (*Id.* ¶ 6). On January 29, 2016, Symantec sold Veritas. (*Id.*). The leased office space was part of the sale, though Symantec continued to sublease the office to Veritas until the end of the lease term on June 30, 2017. (*Id.*; *see also* ECF No. 37 at App052–055). Symantec submits as evidence the lease termination agreement, which became effective on June 30, 2017. (*Id.* at App052–055). Symantec states that it does not have offices at the other addresses provided by CUPP and submits evidence that those addresses do not display any name or logo associated with Symantec. (*Id.* at App002 ¶¶ 2–9). Based on the evidence before it, the Court concludes that Symantec does not have any offices in this District on which venue could be based.

**B. CUPP’s Request for Venue-Related Discovery is Denied.**

CUPP argues it should be able to conduct discovery “to establish the significance of any connections to [Symantec’s] data centers and their physical location.” (ECF No. 34 at 13). CUPP states that further discovery “will lead to evidence that Symantec maintains many more physical locations in this District in addition to the five addresses [already] mentioned” and that “many Symantec employees live and work in this District.” (*Id.* at 12–13). CUPP also asserts that discovery will lead to “information showing Symantec reimburses its employees for home

offices, that its sales employees keep product literature at or conduct business out of their homes, and that they direct sales activities at locations within this District. (*Id.* at 14).

The Court denies CUPP's request for discovery on venue. Symantec does not dispute that its servers are housed at a data center within this District. As discussed above, servers housed in third-party data centers do not meet the venue requirements of § 1400(b). Further, Symantec has provided evidence that none of the addresses CUPP has discovered thus far are associated with Symantec. CUPP has not explained why further discovery has any reasonable prospect of leading to different addresses that are associated with Symantec. Symantec has also presented evidence that it does not reimburse any employees for home offices. The other evidence CUPP expects to obtain with additional discovery would do nothing more than show that "there exists within the district a physical location where an employee of the defendant carries on certain work for his employer," which is not enough to establish venue. *In re Cray*, 871 F.3d at 1366. Because CUPP's proposed discovery on venue would serve no purpose, the Court denies its request.

**C. Transfer to the District of Delaware is in the Interest of Justice.**

Because venue is not proper in the Northern District of Texas, the Court must either "dismiss, or if it be in the interest of justice, transfer [the] case to any district or division in which it could have been brought." 28 U.S.C. § 1406(a). A civil action for patent infringement may be brought in the judicial district where the defendant resides, or where the defendant has committed acts of infringement and has a regular and established place of business. *Id.* § 1400(b). The term "resides" refers only to a defendant's state of incorporation. *TC Heartland*, 137 S. Ct. at 1519.

Symantec argues that the Court should transfer this case to the Northern District of California where the parties' "ties are strongest." (ECF No. 31 at 4). Symantec is headquartered in the Northern District of California and Symantec has filed a declaratory judgment action against CUPP there. (ECF No. 32 at Appx006 ¶ 4, Appx046–057). CUPP requests that the case be transferred to the District of Delaware because Symantec is incorporated in Delaware. (Resp. at 10).

The Court cannot determine whether the Northern District of California is a district in which the case could have been brought because Symantec does not present evidence that it has a regular and established place of business there. The Court finds it is in the interest of justice to transfer this case to the District of Delaware rather than a dismissal. Venue is proper in that district because it is where Symantec resides. *TC Heartland*, 137 S. Ct. at 1519.

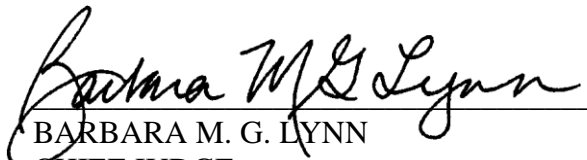
#### **IV. Conclusion**

IT IS ORDERED that Symantec's Motion for Leave to File Appendix in Support of Reply (ECF No. 38) is GRANTED.

IT IS FURTHER ORDERED that Symantec's Motion to Dismiss (ECF No. 31) is GRANTED IN PART and DENIED IN PART. Because venue is improper in the Northern District of Texas, the case shall be transferred to the District of Delaware, pursuant to 28 U.S.C. § 1406(a). The Clerk is directed to close this case after transferring it to the District of Delaware.

**SO ORDERED.**

December 21, 2018.

  
BARBARA M. G. LYNN  
CHIEF JUDGE